INDIAN OVERSEAS BANK

PRESENTS

AWARENESS INCIDENTS BY

IOB ANNA...

(Chapter 7)

(READ IT.....LEARN IT.....USE IT)

"आईओबी अन्ना,
हर दिन चौकन्ना"

Fraud Risk
Management Cell
(Cyber)

"AI (Artificial Intelligence) Voice Cloning Scam" Chapter - 7

AI technology becomes more prevalent in all aspects of life, and it is gradually taking on more sophisticated roles in our society. Along with this not only AI technology becomes smarter, cheaper, and more widely available, but also easier for criminals to incorporate AI technology into their scams. The immense potential of AI is being exploited by cybercriminals, who have harnessed it for malicious purposes, such as creating convincing deepfakes voice and perpetrating unnervingly realistic voice scams. Voice cloning, also called Deepfake voice or synthetic voice, uses AI to generate the speech of a real individual, creating a clone of their specific, unique voice to generate a clone of a person's voice. The technology has advanced to the point that it can closely replicate a human voice with great accuracy in tone and likeness.

Cybercriminals will often source small sample of voice from public social media profiles like You tube, Facebook, Instagram, and other places online where people post about themselves, their families, their travels, and so on.

AI voice cloning is being used by scammers to impersonate as victim's family member or friends or colleagues and deceive victims into giving away money or sensitive information. Using just a few seconds to a minute of data, scammers can use AI software to make a convincing copy of voice and make it say anything they want.

Type of Voice Cloning Scams:

1. **Identity Theft by Voice Cloning (By using Alexa, Siri etc.):**
   Hands-free interaction with our devices is convenient, but voice cloning exposes it as a weak point in our security. Any scammer with access to victim's voice can communicate with victim's devices like Siri and Alexa, which means they may also have access to your credit cards, bank accounts, and personal information.

2. **Fraudulent Phone Calls with Caller ID Spoofing:**
   Between caller ID spoofing and voice cloning, a crafty scammer may have you thinking you are on the phone with your friend or family. The call will come up as their number, and you will hear what sounds like their voice. AI voice cloning allows scammers to casually ask for sensitive information you would only share with friends and family.

3. **Virtual Kidnapping:**
   Scammers may call at home through AI app and some small kid may crying on other side and scammer threaten for ransom or demand for money. At the time family member like aged people may panicked and transfer the money as demanded. But actually, the voice of kid on other side through AI and scammer uses voice cloning for virtual kidnapping.

4. **Links in an Email or Text Message:**
   Many AI voice scams stem from traditional phishing or smishing links. If you find yourself talking to a chatbot after clicking a link in an email or text, you might be in the midst of a scam.

5. **Extraction of Personal Information:**
   In AI voice scam, chatbot might ask you for personal information that is not necessary or relevant to the exchange. Never give out sensitive details like login credentials or financial information without verifying whom you are talking to.

6. **Extreme Situations:**
   AI voice cloning scams can make victims think their loved ones are in serious trouble, and because these situations can be nerve-wracking, it immediately creates a sense of urgency to act upon.

7. **The Voice Banking Scam:**
   The voice banking is also a growing concern where demand for voice-based services for banking and financial transactions increases day by day, which also open doors for scammers for voice cloning scams. In this scam, scammers cloned the voice of victim and communicate with his bank through voice banking for transfer of money to an external account. AI Voice Cloning makes it possible to spoof any person's voice and steal information or money from their bank account.

Scammers stay at the cutting edge of technological advancements, so when a new type of tech is integrated into our culture, scammers integrate it into theirs. Cybercriminals are taking advantage of the accessibility and simplicity of AI voice cloning tools to deceive people into sending money or personal information. Through AI voice cloning scam, anyone and everyone can be targeted. The biggest red flag to watch for is, whom you are talking to ends up asking for the funds or sensitive information. If they ask for a wire transfer, cryptocurrency, gift cards, or other hard ways to track funds, this is a big red flag for AI Voice Cloning Scams. AI voice cloning is the next frontier for fraudsters, and it is up to us to remain alert and how to protect ourselves and our family & friends.

INCIDENT

Anita is a working woman and working in a reputed organization and her son is studying in college. They have a car at home and Anita's son occasionally driving the same. One day Anita received a call from unknown person and unknowingly or due to general tendency she picked up the call.

Hello, who is there!

Hello, I am Rajiv. Your son's vehicle has caused an accident. Please talk to your son.

Perpetrator Mr. Rajiv purportedly pretend that he has handed over phone to Anita's son on other side with malicious intentions.

From other side it is look like Anita's son was crying, and he told to mom that please transfer Rs. 1,00,000/- immediately to settle the matter else I will be in big trouble.

Anita does not understand what happened to her son and the voice on the phone was very much same in tone and she believed that the person on the phone to be her son and he was in big trouble. She got panicked due to distress call and transfer the amount in account provided by perpetrator Mr. Rajiv.

After transfer the money, Anita called on that unknown mobile no. to talk to perpetrator Mr. Rajiv, but that mobile no. is not reachable. She does not understand what to do, so she decided to call her son directly on his mobile no. She called her son and asked about the matter, but her son replied that he is perfectly alright, and he did not meet with any accident.

Anita does not understand matter. She does not understand who called her and who was that person, who talked with her in her son's voice and how it was possible.

Anita immediately called his friend and talked about the matter. Anita's friend was also in shocked, but he suggested Anita to talk to IOB Anna for the matter and assure her that they will definitely help you.

Anita called IOB Anna……

Hello IOB Anna, I am Anita here.

Hello Anita, tell me what happened.

Anna, I got scammed through online, please help me.

I understand Anita, tell me what happened?

Anita narrated the complete incident to IOB Anna.

Anita, I understood your situation and the matter. I also understood that in this type of distress situation it is very hard for you to act calmly. Anita this is new type of online way to defraud the people, generally we call it AI Voice cloning Scam. Anita you have fallen victim to AI Voice Cloning Scam.

Anita, you are defrauded by fraudsters through online AI (Artificial Intelligence) Voice Cloning technology. In AI Voice Cloning Scam, fraudsters have been using fear tactics to try and trick victim into giving away money or sensitive information. Fraudsters are Now using voice cloning technology to create a voice clone of that person and then make distress phone calls sound even more real. Victims answer the call and on the other end of the line victims hear the frantic voice of their loved ones or near ones. AI can equip fraudsters with the tools to make their attacks more convincing, efficient, and fast. The top social media apps where these frauds happened are Facebook, Google Hangouts, Instagram, and WhatsApp.

I am extremely sorry Anna; I did not even know about this. Now what I have to do?

Anita, now immediately lodge a complaint to cyber police station, National Cyber Crime Reporting portal and bank cyber cell team.

Incident Overview by IOB Anna…….

- Anita is the victim of online AI Voice Cloning Scam.
- She reacted on an anonymous call from unknown person.
- She heard the frantic voice of her son on other side, which was not real but due to fear, she immediately transferred the money.
- She never heard about this type of fraud due to this she believed the cloned voice of her son which created by the fraudsters.
- She came in the trap of fraudster by hearing the accident matter, which is general tactics used by fraudsters in AI Voice cloning scam.

Awareness Tips by IOB Anna…….

- Always verify the identity of the caller through another means of communication before taking any action, when it is urgent request.
- Be wary of unexpected urgent requests for money or personal information, even if they appear to come from someone you know.
- Stay informed about different types of online scams and how they work. Awareness is key to preventing falling victim to these scams.
- Stay vigilant and exercise caution in all your interactions over online.
- Be cautious about what you share on social media and other online platforms and set your profiles to “friends and family” only, because scammers can use publicly available information against you convincingly.
- Enable multi factor authentication, if possible, on your financial and important online accounts to add an extra layer of security.
- Please contact at Cyber Police Help Line No. 1930 in case of any cyber fraud.
- Please contact IOB cyber cell at 044 2858 4890 & IOB customer care at 1800 425 4445 or send mail at cybercell@iob.in in case of cyber payment fraud.

AI Voice is an Overt Peril, Stay Alert!!

इण्डियन ओवरसीज़ बैंक
Indian Overseas Bank
आपकी प्रगति का सच्चा साथी
Good people to grow with

FRMC

“AI Voice cloning is a boon for everyone, Artist uses for Raise & Con-Artist uses for Raze”

“Scammers are Using AI Voice Cloning to Dupe the People,

Because They Know,

It is Easy to Dupe People

Instead of Duping the System”

THANKS!